ERRATA 1
To
SCA Security Supplement V1.0

13 July 2001

The following changes have been authorized by the JTRS Change Control Board as approved Change Proposals 142, 380, 383, 416, 469, and 475.

Change the cover page as follows:

change the version number to read: V1.1

change the date to read: July 13, 2001

Add a new line to theRevison Summary table, as shown below:

1.1	Incorporate approved Change Proposals, numbers 142, 380, 383, 416, 469, 475

Change the list found in section 3.3.1.4 to read:

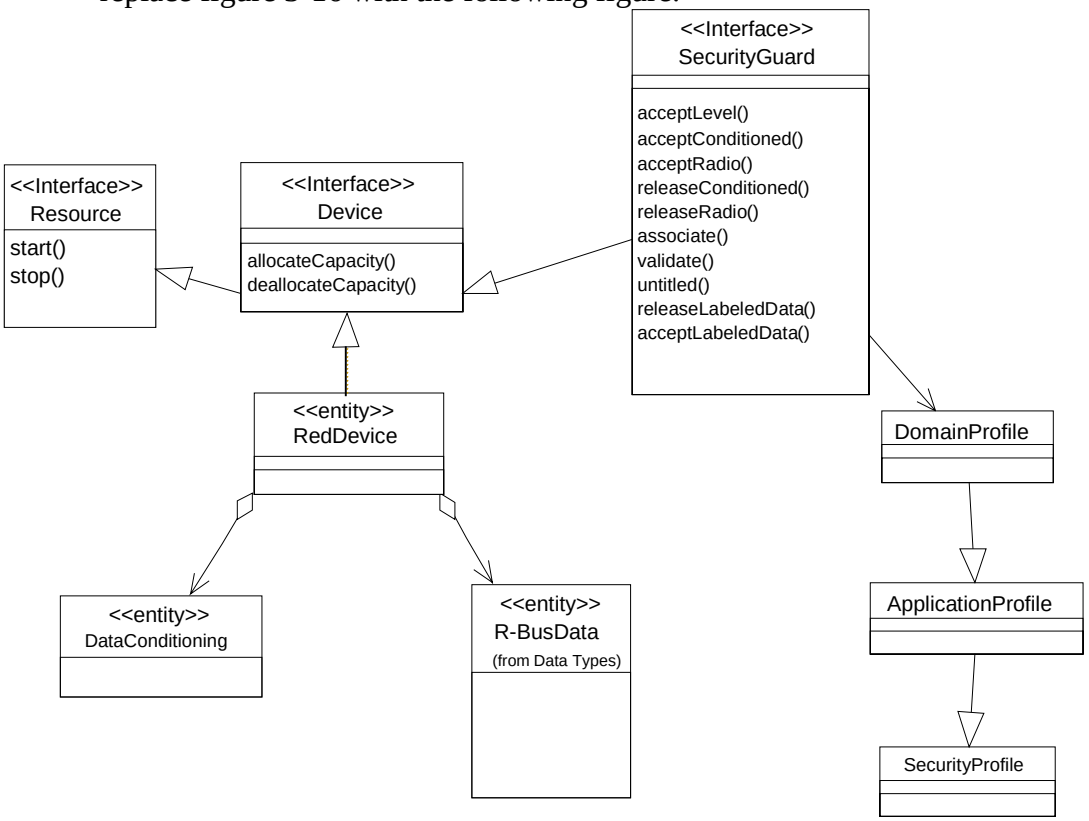
- *DomainManager*
- *Device*
- *LoadableDevice*
- *ExecutableDevice*
- Domain Profile
- *ApplicationFactory*
- *ResourceFactory* (optional)
- Audit
- *FileSystem*
- *FileManager*

Change the list found in section 3.6.3 to read:

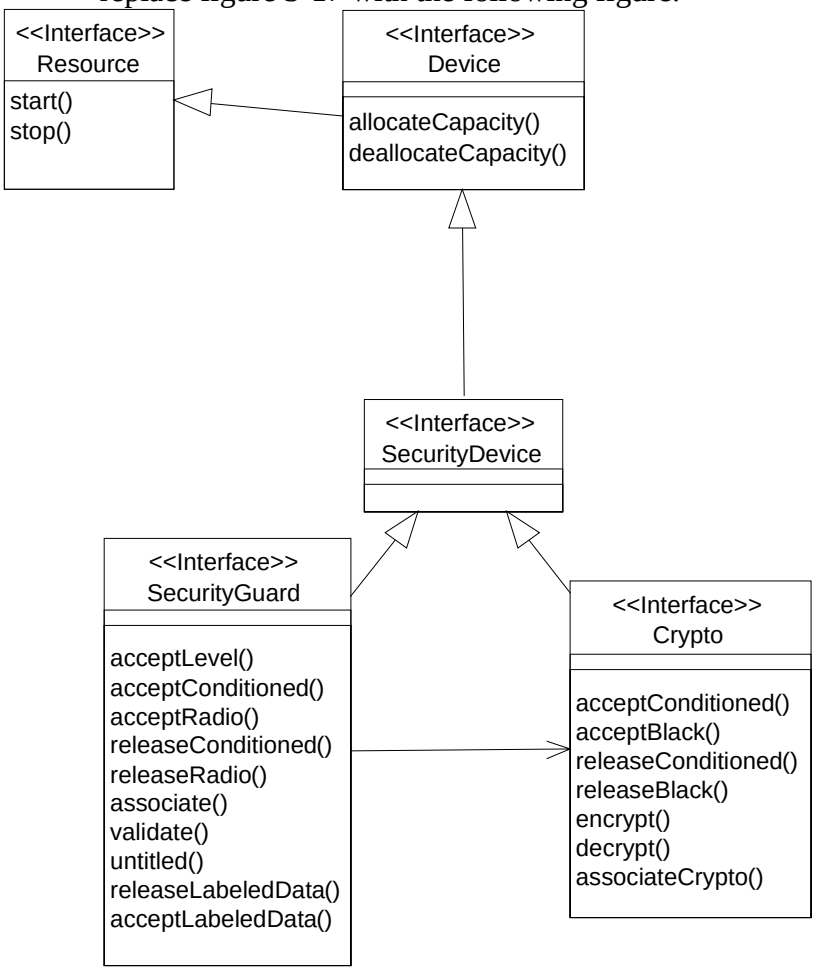
- *DomainManager*
- *Device*
- *LoadableDevice*
- *ExecutableDevice*
- Domain Profile
- *ApplicationFactory*
- *ResourceFactory* (optional)
- *FileSystem*
- *FileManager*

Change the following two figures in section 3.6.4.2:

replace figure 3-16 with the following figure:



replace figure 3-17 with the following figure:



Change item 2, in section 4.1.2 to read:
The CS/S of the Security Architecture shall have a minimum Common Criteria rating of EAL4.

Change item 3, in section 4.1.2 to read:
The INFOSEC Boundary Component of the Security Architecture (security functions outside of the CS/S) shall have a minimum Common Criteria rating of EAL3.

Change section 4.3.1.2 to read:
The general requirements placed upon the INFOSEC Boundary are stated in section 4.1.2.

Change item 7, in section 4.3.2.2 to read:
The process separation mechanism shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures).

Change item 8, in section 4.3.2.2 to read:
The process separation mechanism shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

Change item 7, in section 4.3.3.2 to read:
The access control mechanism shall exist in a domain separate from user applications that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the entity may be a defined subset of the subjects and objects in the processing system.

Change item 8, in section 4.3.2.2 to read:
The access control mechanism shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

Changes to section 4.3.5.2 are as follows:

delete item 2, including its text (text to delete is shown below).
"2. No information, including encrypted representations of the information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system."

renumber item 3 to be item 2 and change its text to read:
"2. The JTR shall clear all memory used to store classified traffic prior to instantiating lower classifications of system high."

renumber item 4 to be item 3 and change its text to read:
"3. The JTR shall clear all memory used to store classified traffic prior to instantiating channels of different system high type classification."

Change the final paragraph, in section 4.3.7.2.1, to read:
"The HMI security policy enforcement mechanism (guard) is much like other application-level, security policy enforcement mechanisms within the JTRS. See figure 4-12. The HMI security policy enforcement guard relies on a protected process space to protect object references for a system high implementation. The intent of the HMI security policy enforcement guard is to restrict an Operator/Administrator/Security Operator/Maintainer access to system and communicator information, and to functionality within the JTRS. The authentication portion of the HMI security policy depends on the mission and application for its use."

Delete item 8, including its text, in section 4.3.7.2.2. The text that is to be deleted did read as follows:
"8. The authentication requirement shall be mission and application specific."

Changes to section 4.3.7.3.2 are as follows:

change the text of item-7 to read:
"7. The installer software shall replace the digital signature on downloaded files with an integrity check (e.g. CRC) after the digital signature has been verified and prior to placement in accessible storage.

change the text of item-9 to read:
"9. The installer application shall provide the capability to install Security Policy files.

Add the following two requirements as items 10 and 11:

"10. The installer shall use the Integrity and Authentication services of the JTRS Security API for the purpose of authenticating digitally signed files and checking their integrity.

11. The installer shall use the Crypto services of the JTRS Security API for the purpose of encrypting and decrypting downloaded files."

Change the final paragraph, in section 4.3.7.4.1, to read:
"The ability to set priorities for audit events and actions that might be taken is necessary. It is noted that the audit function is not part of any policy enforcement function. The audit feeds applications that can act on information delivered. The implementation of Audit is dependent upon the operational environment and the equipment being used for that mission."

Changes to section 4.3.7.4.2 are as follows:

change the text of item-3 to read:
"3. An administrator or security officer shall be able to:
a. Select the types of events that the audit function will collect and report
b. Determine user access to the various event types."

change the text of item-4d to read:
"d. The audit mechanism shall collect information on violations of the CS/S bypass security policy."

change the text of item-4e to read:
"e. The audit mechanism shall collect information on violations of access control security policy"

delete item 5, including its text. The text that is to be deleted did read as follows:
"5. Audit requirements shall be operationally determined depending on equipment and mission."

renumber item 6 to now be item 5.

renumber item 7 to now be item 6.

Change section 4.4.1.1 to read:
4.4.1.1 TEMPEST Requirements.
The requirements for TEMPEST will be established by individual procurements and can be found in the Unified INFOSEC Criteria (UIC).

Change section 4.4.2.1 to read:
4.4.2.1 Tamper Requirement.
The requirements for TAMPER will be established by individual procurements and can be found in the Unified INFOSEC Criteria (UIC).

Change section 4.4.3.1 to read:
4.4.3.1 Electrical Protection Requirement.
The guidelines/requirements will be established by the individual procurements and can be found in the Unified INFOSEC Criteria (UIC).

Delete item 2, including its text, in section 4.6.2.1. The text that is to be deleted did read as follows:
"2. The requirement for installation is that the security APIs be used to validate digital signatures."

Change item 1, in section 4.6.3.1 to read:
A test shall be executed that validates the correct operation of the red and black portions of the bypass individually prior to a cooperative red/black bypass test.